Membership Services Department
500 Montgomery Street
Suite 700
Alexandria, Virginia 22314-1561
Phone: (703) 739-0300
FAX: (703) 836-1608
WEB: http://www.pcia.com

Standard 2

CALEA Specification for Advanced Messaging

Version 1.0

PCIA Technical Committee

CALEA Subcommittee

25 August, 1998

Chairs:

CALEA Subcommittee: David I. Odom, DOdom@conxus.com (CONXUS Communications, Inc.)
Regulatory Working Group: David I. Odom, DOdom@conxus.com (CONXUS Communications, Inc.)
Technical Working Group: Joe Mullin, JMullin@archcomm.com (Arch Communications Group, Inc.)

Authors:

Stephen Oshinsky, soshinsky@mtelatc.com (SkyTel Communications, Inc.)
Rob Lockhart, rob.lockhart@mot.com (Motorola, Inc.)
Garland Phillips, FGP004@email.mot.com (Motorola, Inc.)
John Davis, jdavis@pagemart.com (PageMart Wireless, Inc.)
Ron Mercer, ron@email.rtswireless.com (Real Time Strategies Inc.)
Dave Mook, ralph@teknow.com (TekNow, Inc.)
Barry Kanne, barry@tga.com (TGA Technologies, Inc.)

Contributors:

Deb Peterson, deb.peterson@ammobile.com (American Mobile)
Rod Massie, rod.massie@ammobile.com (American Mobile)
Tony Phipps, tphipps@vancouver.glenayre.com (Glenayre Technologies Inc.)
Adnan Saleem, asaleem@glenayre.com (Glenayre Technologies Inc.)
Greg Wells, Gwells@atlanta.glenayre.com (Glenayre Technologies Inc.)
Steven Day, day@metrocall.com (Metrocall, Inc.)
Mark Witsaman, mwitsaman@mobilecomm.com (MobileMedia Communications Inc.)
Mike Sheffield, msheffield@mtelatc.com (SkyTel Communications, Inc.)
Richard Dietz, FRD006@email.mot.com (Motorola, Inc.)
Jody Montinola, CJM043@email.mot.com (Motorola, Inc.)
James Lacey, JDL6972@email.mot.com (Motorola, Inc.)
Steven Petit, CSP005@email.mot.com (Motorola, Inc.)
Vick Cox, vcox@pagemart.com (PageMart Wireless, Inc.)
Chris Ward, cward@corp2.pagemart.com (PageMart Wireless, Inc.)
Keith Kornfeld, keith@rtswireless.com (Real Time Strategies Inc.)
Rob Hoggarth, hoggartr@pcia.com (PCIA)
Eddie Gleason, gleasone@pcia.com (PCIA)
Donald Vasek, vasekd@pcia.com (PCIA)

Editor:

Rob Lockhart, rob.lockhart@mot.com (Motorola, Inc.)

Document Status:

1.0   First publication (980825)

Trademarks, Registered Trademarks, and Service Marks:

Copyright:

Foreword

In this document, the Personal Communications Industry Association (PCIA) Technical Committee defines the specifications for interface compatibility requirements between paging or wireless packet data service providers (PSPs) and law enforcement agencies (LEAs) for Advanced Messaging services.

Advanced messaging services include such services as subscriber defined on-demand roaming, forwarding and redirection, two-way and acknowledged voice paging, and wireless packet data services.

The Communications Assistance for Law Enforcement Act (CALEA)[1] was enacted on October 25, 1994. CALEA requires telecommunications carriers to ensure that their equipment, facilities, or services have the capability to:

(1) "expeditiously ... isolate and enable the government to intercept all communications in the carrier's control to or from the equipment facilities or services of a subscribe[r], concurrently with the communications' transmission, or at any later time acceptable to the government;"

(2) "expeditiously ... isolate and enable the government to access reasonably available call identifying information about the origin and destination of communications;"

(3) "make intercepted communications and call identifying information available to government in a format available to the carrier so they may be transmitted over lines or facilities leased or procured by law enforcement to a location away from the carrier's premises;" and

(4) "meet these requirements with a minimum of interference with the subscriber's services and in such a way that protects the privacy of communications and call identifying information that are not targeted buy [sic] electronic surveillance orders, and that maintains the confidentiality of the government's wiretaps."[2]

Under CALEA, industry associations and standards-setting bodies are authorized to adopt standards for satisfying these assistance capability requirements. Telecommunications carriers, manufacturers, and/or support service providers that comply with these standards have "safe harbor" and are deemed in compliance with CALEA's capability requirements:

"a telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found in compliance with section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization. ..."[3]

---

[1] Communications Assistance for Law Enforcement Act, Pub. L. No 103-414 (CALEA).

[2] Telecommunications Carrier Assistance to the Government, H. Rep. No. 103-827, at 22 (October 4, 1994).

[3] CALEA, § 107.

In November 1997, an Interim Standard (J-STD-025) for wireline and wireless te-
lephony was adopted by the Telecommunications Industry Association Subcommit-
tee TR45.2 and Committee T1 of the Alliance for Telecommunications Industry So-
lutions.[4] Shortly thereafter, in December 1997, a working group was established un-
der the auspices of PCIA to determine whether J-STD-025 was readily applicable to
paging or wireless packet data technology and, if not, to develop a separate stan-
dard for the paging and wireless packet data industry. After carefully reviewing J-
STD-025, the working group determined that J-STD-025's telephony specifications
were not readily applicable to paging or wireless packet data technology and that a
separate standard was necessary.

In order to expedite the standards-setting process, the Paging Technical Committee
decided to develop a Suite of Standards and release this Suite of Standards in
three parts. This Standard deals with Advanced Messaging. Any PSP, manufac-
turer, or service provider that complies with this Standard will have "safe harbor" for
Advanced Messaging services under section 107 of CALEA and will be found in
compliance with CALEA's assistance capability requirements.

The following Standard for advanced messaging services supplements the standard
previously adopted for traditional, one-way paging services[5].

One annex is attached to this standard. This annex is informative only and is not a
part of this standard.

---

[4]   Lawfully Authorized Electronic Surveillance, TIA/ATIS, Interim/Trial Use Standard (J-STD-025).

[5]   Standard 1, CALEA Specification for Traditional Paging, v1.0

Document Change Record

v1.0   25 August, 1998   First release of document.

Table of Contents

Table of Figures

1.   Introduction

In this document, the PCIA Technical Committee defines the specifications for interface compatibility requirements between PSPs and LEAs for Advanced Messaging services.

Advanced messaging services include such services as subscriber defined on-demand roaming, forwarding and redirection, two-way and acknowledged voice paging, and wireless packet data services.

The following Standard for advanced messaging services supplements the standard previously adopted for traditional, one-way paging services.

One annex is attached to this standard. This annex is informative only and is not a part of this standard.

1.1   Purpose

In this document, the PCIA Technical Committee defines the specifications for interface compatibility requirements between PSPs and LEAs for Advanced Messaging services.

Any PSP, manufacturer, or service provider that complies with this Standard will have "safe harbor" for Advanced Messaging services under section 107 of CALEA and will be found in compliance with CALEA's assistance capability requirements.

1.2   Scope

The scope of this Standard is to define the services to support LAES and the interface between a PSP and an LEA for Advanced Messaging services.

1.3   How This Document is Organized

This Standard is organized as follows:

Foreword provides an overview of this document.

Document Change Record provides revision control for this document.

Section 1   **Introduction** defines the purpose, scope, and organization of this document.

Section 2   **Features and Services Overview** defines the means to access Advanced Messaging communications through the means of an independent communications path.

Section 3   **Assumptions** identifies this Standard's assumptions related to call content and reasonably available call-identifying information.

Section 4   **Network Reference Model** identifies the set of functional entities and actions for the intercept process.

Section 5   **Call Content and Reasonably Available Call-Identifying Information Delivery** describes the information provided by the PSP Infrastructure Data Delivery Point for LEA(s).

Section 6   **Call Content and Reasonably Available Call-Identifying Information Surveillance Service Description** describes the service provided by the PSP Infrastructure to deliver call content and reasonably available call-identifying information for a particular intercept subject.

Section 7   **Advanced Messaging Interface (AMI) Protocol** defines the protocol used to deliver call content and reasonably available call-identifying information from the PSP Infrastructure Data Delivery Point for LEA(s) for use by the LEA-Provided CALEA Interface.

References   References defines a list of the references used in the preparation of this Standard.

Glossary   Glossary defines the words, acronyms, and initialisms that are used in this Standard.

Annex 1   **Examples** gives a non-comprehensive list of illustrative uses of this Standard.

2. Features and Services Overview

This Standard defines intercept of wireless communications for subjects equipped with "Advanced Messaging" services. The following describes the operational features and capabilities of the services classified as "Advanced Messaging".

2.1 Advanced Messaging Services

Advanced messaging services, as currently perceived, are:

2.1.1 Subscriber Defined On-Demand Roaming

Subscriber defined on-demand roaming permits the subscriber to change the geographic radio coverage area of the PSP's infrastructure to which the subscriber's outbound messages are to be sent.

2.1.2 Forwarding and Redirection

Forwarding and redirection permits the subscriber to change the destination radio device or specify an external address which is alerted by outbound message calls to the subscriber's given access number, PIN, or capcode.

2.1.3 Two Way and Acknowledged Voice Paging

Two-way and acknowledged voice paging are advanced wireless services that support the transmission of tone-only, numeric, alphanumeric, binary data, and voice message signals between control terminals at fixed location(s) and radio transceiving devices.

There are two basic types of intercept subject-related content and call-identifying information transactions associated with these services:

Outbound Messages

Outbound messages are transmitted to the radio transceiving device from the radio transceiving device's Home Node within the PSP Infrastructure. These messages may originate from external wireline sources, other wireless devices, or the PSP Infrastructure.

Inbound Messages

Inbound messages are transmitted by the radio transceiving device to the radio transceiving device's Home Node within the PSP Infrastructure. These messages may be destined for external wireline addresses, other wireless devices, or the PSP system.

2.1.4 Wireless Packet Data Services

Wireless Packet Data Services are advanced wireless data services that support the transmission of numeric, alphanumeric, and binary packet data message signals between control terminals at fixed location(s) and radio transceiving devices.

There are two basic types of intercept subject-related content and call-identifying information transactions associated with these services:

Outbound Messages

Outbound messages are transmitted to the radio transceiving device from the radio transceiving device's Home Node within the PSP Infrastructure. These messages may originate from external wireline sources, other wireless devices, or the PSP Infrastructure.

Inbound Messages

Inbound messages are transmitted by the radio transceiving device to the radio transceiving device's Home Node within the PSP Infrastructure. These messages may be destined for external wireline addresses, other wireless devices, or the PSP system.

2.2   Advanced Messaging Interface Advantages

The Advanced Messaging Interface techniques included in this Standard for advanced messaging services offer a number of advantages.

Inclusive - The Standard addresses all currently perceived Advanced Messaging services including advanced one-way and both the outbound and inbound portions of two-way paging, acknowledged voice, and wireless packet data,

Universal -Can be implemented using industry-standard computer protocols,

Uniform - A single interface standard supports both large and small LEAs,

Scaleable - Cost-effective for small systems and LEAs and may be field-expanded as needs grow,

Discrete - Invisible to both intercept subjects and callers and controlled visibility to PSP staff,

Connectivity - Flexible data transmission protocol delivers surveillance on tone-only, numeric, alphanumeric, binary data, and voice messages over the most appropriate communications facilities.

3.   Assumptions

This Standard for advanced messaging is based upon the following assumptions.

3.1   General

Advanced Messaging LAES capabilities allow a PSP to deliver the intercepted call content and reasonably available call-identifying information, associated with completed paging or wireless packet data calls to subscriber accounts which are equipped for Advanced Messaging services, to an authorized LEA via the most appropriate communications facilities.

3.2   Call Content

Although not specifically defined in CALEA, "content" is defined in 18 USC 2510 (8) to be "when used with respect to any wire or electronic communications, includes any information concerning the substance, purport or meaning of that communication." As interpreted by this Standard for advanced messaging, call content covers tone-only, numeric, alphanumeric, binary data, and voice messages:

> Delivered to the PSP RF Network or to the appropriate External Messaging source or Input Node when termination is applicable and the alternate address is an external wireline address from the subscriber's Home Node in the PSP Infrastructure in advanced one-way, two-way, acknowledged voice, and wireless packet data outbound message services, or

> Transmitted from a subscriber's radio transceiving device and delivered to the subscriber's Home Node in the PSP Infrastructure in advanced two-way, acknowledged voice, and wireless packet data inbound message services.

Call content information supplied by the PSP to the LEA may be derived from multiple sources (email, multiple phone/pin numbers, etc.). The PSP will, under the terms of a Lawful Authorization, provide all reasonably available information to the LEA.[6] It shall remain the responsibility of the LEA to review and minimize any delivered information which falls outside the bounds of the Lawful Authorization.

3.2.1   Encryption

As interpreted by this Standard for advanced messaging, encryption is defined as the process of changing the format of the information content of a message or message routing information such that external observers will not be able to interpret correctly the content or routing information.

A PSP shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the PSP, and the PSP possesses the information necessary to decrypt the communication.[7]

---

[6]   47 U.S.C. § 2518(4) does not mandate that a Lawful Authorization authorizing the interception of a subscriber's facilities identify those facilities in any specific manner (e.g., by the phone number associated with that facility as opposed to the capcode and frequency for the facility). Instead, it simply requires that the order specify "the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted."

[7]   CALEA, § 103(b)(3).

3.2.2   Encoding

As interpreted by this Standard for advanced messaging, encoding is defined as the conversion of data or voice signals into a format suitable for transmission by the PSP infrastructure.

If the PSP Infrastructure encodes data or voice, then the encoding algorithm will be made available to the LEA if appropriate. Licensing issues associated with such encoding formats are beyond the scope of this Standard and must be handled between the LEA and the licensor.

3.2.3   Compression

As interpreted by this Standard for advanced messaging, compression is defined as the reduction in the number of bits required to exchange information between two or more parties.

If the PSP Infrastructure compresses data or voice, then the compression algorithm will be made available to the LEA, if appropriate. Licensing issues associated with such compression methods are beyond the scope of this Standard and must be handled between the LEA and the licensor.

Compression can take on multiple forms as illustrated by the following examples.

> **Codes** - where a code of 01 may represent a character string comprised of one or more words,
>
> **Abbreviations** - where common words are abbreviated such as "PLZ" for "Please", and
>
> **Compression of binary data** - where a lossless or lossy algorithm is used to reduce the redundant information content in a message.

If the PSP Infrastructure compresses a message using codes or abbreviations, then the PSP Infrastructure will decompress the message prior to sending it to the LEA.

If the PSP Infrastructure compresses a message using a lossless or lossy compression algorithm, then the compression algorithm will be made available to the LEA. If a lossy compression algorithm is used on the call content, no translations of content will be provided as part of the Delivery process to the LEA so as to protect the integrity of information content of the message. Licensing issues associated with such algorithms are beyond the scope of this Standard and must be handled between the LEA and the licensor.

3.3   Call Identifying Information

Call identifying information is defined in CALEA Section 102 (2) to be "dialing or signaling information that identifies the origin, direction, destination or termination of each communication generated or received by a subscriber by means of any equipment, facility or service of a [PSP]".

3.3.1   Outbound Message Services

As interpreted for advanced one-way, two-way, acknowledged voice, and wireless packet data outbound message services by this Standard for advanced messaging, outbound message services call-identifying information is defined as follows:

Destination is the radio receiving or transceiving device address to which a call is being made (e.g., called party);

Direction is the outbound transmission path from the PSP Home Node to the RF network or to the appropriate External Messaging source or Input Node when termination is applicable and the alternate address is an external wireline address;

Origin is the number or address of the party initiating the call (e.g., calling party); and

Termination is the alternate address to which a call is being routed, if applicable (e.g., forwarded party).

For these outbound message services, reasonably available call-identifying information is that information used in the Home Node for call processing. Reasonably available call-identifying information generally consists of the address of the subject's radio receiving or transceiving device(s) and, if appropriate, the address to which the message has been forwarded or redirected. The call origin is not reasonably available in most PSP installations but may be obtained through the originating service provider (e.g., EC, ISP).

3.3.2 Inbound Message Services

As interpreted for advanced two-way, acknowledged voice, and wireless packet data inbound message services by this Standard for advanced messaging, inbound message services call-identifying information is defined as follows:

Destination is the number or address of the device to which the intercept subject sends a message (i.e., called party),

Direction is the transmission path from the intercept subject's radio transceiving device to the intercept subject's PSP Home Node,

Origin is the address of the intercept subject's radio transceiving device sending the message (i.e., the calling party), and

Termination is the same as *Destination*.

For these inbound message services, both *Origin* and *Destination* information are available.

3.4 Call Completion

As interpreted by this Standard for advanced messaging, call completion is defined as follows:

Delivery, from the Home Node, of the tone-only, numeric, alphanumeric, binary data, and/or voice messages to the RF network or to the appropriate External Messaging source or Input Node when termination is applicable and the alternate address is an external wireline address in advanced one-way, two-way, acknowledged voice, and wireless packet data outbound message services,

Arrival, at the Home Node, of the tone-only, numeric, alphanumeric, binary data, and/or voice messages transmitted from a subject's radio transceiving device in advanced two-way, acknowledged voice, and wireless packet data inbound message services. Any transmissions attempted by a subject's radio transceiving device which do not arrive at the Home Node are not considered to be "completed".

3.5   PSP Infrastructure Architectural Model

As interpreted by this Standard for advanced messaging, the PSP Infrastructure ar-
chitecture is defined to include three distinct network nodes as shown in Figure 1.
These nodes are defined as follows:

> **Input Node** encompasses those functions needed to deliver messages to and
> from wireline carrier sources (e.g., EC, ISP),

> **Home Node** encompasses subscriber database records and those functions
> needed to route messages between the appropriate Input Node(s) and the
> RF Network, and

> **RF Network** encompasses those functions needed to deliver messages to
> and from wireless carrier sources (e.g., radio transceiving devices). The RF
> Network includes RF transmitters and Output Node encoders and, in two-way
> advanced messaging systems, RF receivers.

These network nodes may be geographically distributed or concentrated and may
exist as either individual physical or virtual entities or some combination thereof.
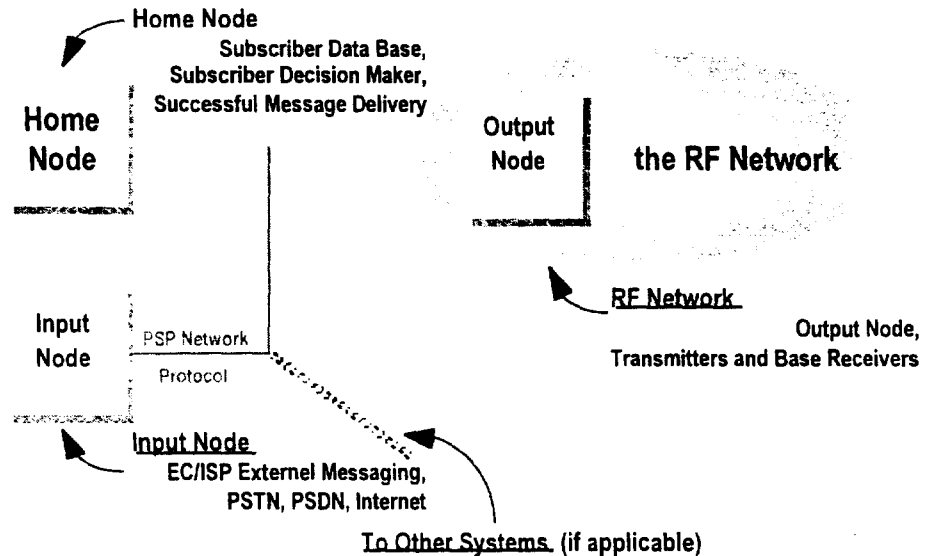

Figure 1:   Single System PSP Infrastructure Model

These network nodes may also be grouped to form a PSP Infrastructure consisting of multiple system nodes. One such multiple system PSP Infrastructure is shown in Figure 2.

Single System #1

| Home Node | | Output Node | the RF Network |

| Input Node | |

Single System #2

| Home Node | | Output Node | the RF Network |

| Input Node | |

PSP Network Protocol

To Other Systems (if applicable)

Single System #N

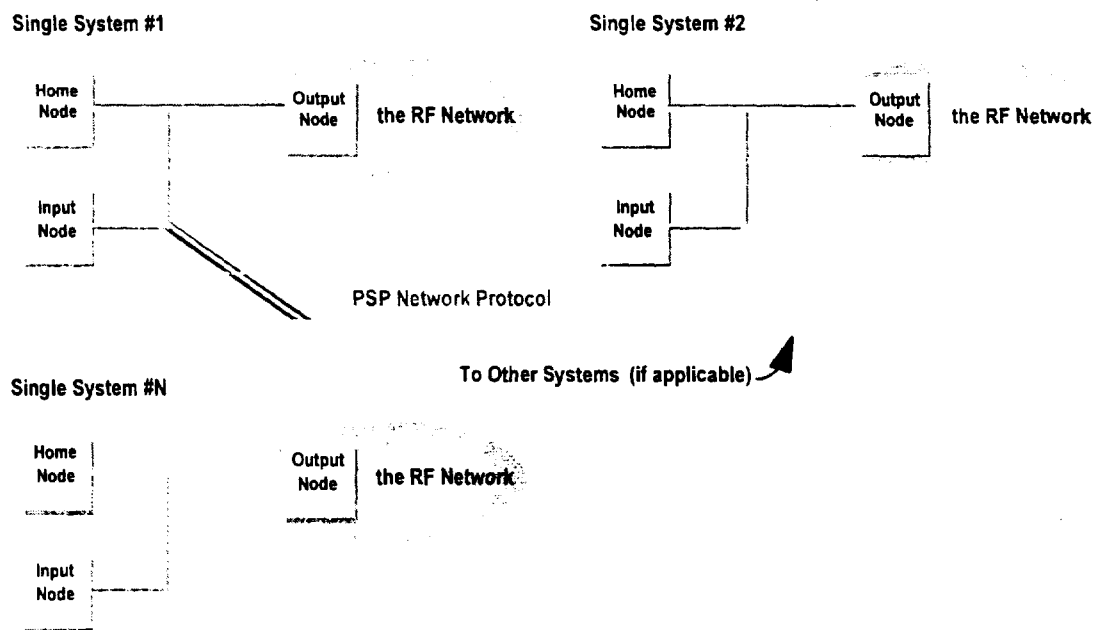| Home Node | | Output Node | the RF Network |

| Input Node | |

Figure 2:   Multi-System PSP Infrastructure Model

The definition of the functions of these network nodes and any or all protocols used between these network nodes is beyond the scope of this Standard.

4.   Network Reference Model

The intercept process consists of a set of functional entities and the actions be-
tween the functional entities. The functional entities (PSP Administration, LEA
Administration, LEA-Provided CALEA Interface, PSP Infrastructure, and External
Messaging) provide the functions of the system and actions (Authorization, Provi-
sion, and Delivery) provide the communication of information between the func-
tional entities. These actions and functional entities are discussed without regard to
their implementation. The relationships between these actions and functional enti-
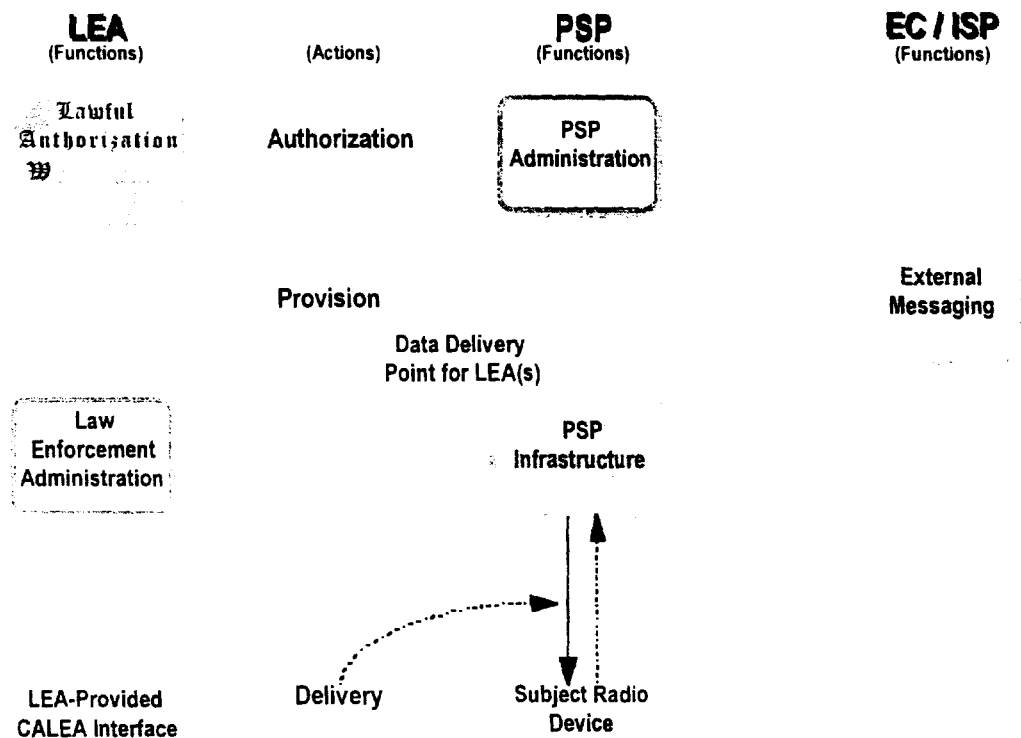ties are shown in Figure 3.

Figure 3:   Advanced Messaging Intercept Model

The **Lawful Authorization** is an important part of the LAES. No intercepts shall take
place without specific lawful authorization. One Lawful Authorization may encom-
pass multiple devices and/or multiple geographic locations.

4.1   Lawful Authorization Action

The Lawful Authorization Action is the serving of the Lawful Authorization to the
PSP by the LEA.

4.2   PSP Administration Function

The PSP Administration Function is responsible for controlling the Provision, ena-
bling the Delivery Actions, and maintaining the Data Delivery Point for LEA(s).

Other functions of the PSP Administrative Function are beyond the scope of this
standard.

4.3   Provision Action

The Provision Action is responsible for enabling and disabling activation of the Data Delivery Point for LEA(s). The Provision Action includes the ability:

> to unobtrusively make the call content and reasonably available call-identifying information available to the delivery action and

> to protect (i.e., prevent unauthorized access, manipulation, and disclosure) intercept controls and intercepted call content and reasonably available call-identifying information consistent with PSP security policies and practices.

For advanced messaging, the Provision Action establishes the interface and controls between the LEA and the PSP for the purpose of intercepting messaging traffic as specified by a Lawful Authorization.

4.4   Law Enforcement Administrative Function

The Law Enforcement Administrative Function is responsible for controlling LEA electronic surveillance functions.

The LEA is also responsible for providing the LEA-Provided CALEA Interface and the associated Delivery Function link to the PSP Infrastructure Data Delivery Point for LEA(s) for receiving the messaging traffic of the subject of a lawful authorization and for transporting, capturing, and processing of the delivered call content and reasonably available call-identifying information.

The Law Enforcement Administrative Function is the responsibility of the LEA.

Other functions of the Law Enforcement Administrative Function are beyond the scope of this standard.

4.5   External Messaging Function

The External Messaging Function is the delivery of messages to and from wireline carrier sources (e.g., EC, ISP) to the PSP Infrastructure and is beyond the scope of this Standard.

4.6   PSP Infrastructure Function

The PSP Infrastructure Function is the switching and radio transmission network of the PSP. For this Standard, the PSP Infrastructure is responsible for the collection and delivery of call content and reasonably available call-identifying information of one or more lawfully authorized intercept subject(s). The PSP Infrastructure function includes the ability:

to accept reasonably available call identifying information for each inter-cept subject for each message received by the home node;

to accept call content for each intercept subject received by the home node;

to gather the information required for providing the reasonably available call-identifying information consisting of the message origin (if reasonably available), message destination, message termination (if appropriate), and date and time of successful message delivery to the RF Network (when the direction is to the Intercept Subject from the PSP Infrastructure) and suc-cessful message delivery to the Home Node of the Intercept Subject (when the direction is from the Intercept Subject to the PSP Infrastructure) and call content;

to ensure that the call content and reasonably available call-identifying in-formation delivered from the Data Delivery Point for LEA(s) is authorized for a particular LEA;

to deliver the call content and reasonably available call-identifying informa-tion for each intercept subject from the Data Delivery Point for LEA(s) for use by one or more LEA-Provided CALEA Interfaces (up to a total of five per in-tercept subject);

to ensure that delivery is only available from the Data Delivery Point for LEA(s) for the time limit bounds set by the Lawful Authorization; and

to protect (i.e., prevent unauthorized access, manipulation, and disclosure) intercept controls and intercepted call content and reasonably available call-identifying information consistent with PSP security policies and prac-tices.

4.7 Delivery Action

The Delivery Action is responsible for delivering intercepted communications expe-ditiously from the PSP Infrastructure Data Delivery Point for LEA(s) for use by one or more LEA-Provided CALEA Interfaces (up to a total of five per intercept subject). Transporting, capturing, and processing of the delivered call content and reasona-bly available call-identifying information is the responsibility of the Law Enforce-ment Administrative Function.

The Delivery Action includes the ability:

to deliver call content and reasonably available call-identifying information for each intercept subject from the PSP Infrastructure Data Delivery Point for LEA(s) and

to protect (i.e., prevent unauthorized access to, manipulation of, or disclo-sure of) intercept controls and intercepted call content and reasonably available call-identifying information consistent with PSP security policies and practices.

For advanced messaging, the Delivery Action delivers call content and reasonably available call-identifying information using the Advanced Messaging Interface (AMI) Protocol from the PSP Infrastructure Data Delivery Point for LEA(s) for use by the LEA-Provided CALEA Interface.

Enabling and disabling the Delivery Function from the PSP Infrastructure Data De-livery Point for LEA(s) as defined in the Lawful Authorization is the responsibility of the PSP.

The methods of delivery transport (e.g., Ethernet, X.25, Dial-Up PPP, Frame Relay) and security measures (e.g., SSL, dedicated transmission paths, ACE Card access on Dial-Up PPP) employed by the LEA are beyond the scope of this Standard.

4.8   Subject Radio Device Function

The Subject Radio Device Function is responsible for collecting and interpreting communications from and, where applicable, encoding and disbursing communications to the Home Node of the intercept subject.

The functions of the Subject Radio Device are beyond the scope of this Standard.

4.9   LEA-Provided CALEA Interface Function

The LEA-Provided CALEA Interface Function is responsible for collecting lawfully authorized intercepted communications (i.e., call content and reasonably available call-identifying information) for the LEA. The LEA-Provided CALEA Interface Function is the responsibility of the LEA.

The LEA-Provided CALEA Interface Function includes the ability to receive and process call content and reasonably available call-identifying information for each intercept subject as delivered using the Advanced Messaging Interface (AMI) protocol.

Enabling and disabling of the activation of the LEA-Provided CALEA Interface is the responsibility of the LEA Administration Function and is beyond the scope of this Standard.

Procurement and monitoring of the LEA-Provided CALEA Interface is the responsibility of the LEA and is beyond the scope of this Standard.